IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Hybrid DCT-DWT Digital Image Steganography

Anuradha Goswami[1], Sarika Khandelwal[2]

M. Tech. Scholar (CSE), Geetanjali Institute of Technical Studies, Udaipur (Raj) India [1]

Assistant Professor, Department of CSE, GITS, Udaipur (Raj) India[2]

Abstract: Steganography is the Method of hiding secret information in a multimedia carrier as image file, audio file and video file. This differs from cryptography concept which is applied to make a message unreadable by a third party but does not hide the existence of the secret communication. Research issues in Image steganography are to increase efficiency in term of the payload capacity of secret information, robustness against visual attacks and statistical attacks. Image steganography in Wavelet transform domain have higher robustness against statistical attacks compared to image steganography in spatial domain and Discrete Cosine Transform domain, While DCT image steganography have higher imperceptibility compared to DWT image steganography. The combined technique of DWT and DCT provides advantages of both techniques. The Proposed algorithm presents Hybrid DCT-DWT Digital image steganography algorithm. Proposed Approach embedding image is embedded is imperceptible part of an image than other methods as shown in results. Steganography is done by embedding image in middle frequency coefficient set of the 3-level DWT transform of host image followed by block DCT transformation and embedding in selected HH DWT coefficient sets.

Keywords: Steganography, Digital image, DCT, DWT, PSNR

I. INTRODUCTION

A. Steganography

Steganography is the art of hiding secret message in to cover medium. The steganography process generally involves placing a hidden message in some transport medium called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. The objective of a teganography is to hide a message from a third party in communication [1].

This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing. Unlike cryptography which is about protecting the secret data, steganography is to conceal existence of the secret data.

Steganography is a practice of imperceptibly altering a work (image, audio, code or hardware) to embed a message about that work itself. Digital media steganography is content specific and the proposed method incorporates visual cryptography with multiple frequency transform based steganography models to enhance the robustness. Importance of steganography has been noticed since early days [2].

Unlike cryptography which is about protecting the secret data, steganography is to conceal existence of the secret data. Steganography (stego = covered + graphy = writing) means covered writing. A sender wants to share a secret message m with other person. He selects randomly a potentially unuseful message or a cover object C. The message to be shared is then embedded into C, by using a key K (called stego-key), and the transformed output is called stego object S. This stego object is shared with receiver without raising any suspicion to the eavesdropper. The extraction process should not need any knowledge of the cover object .So the security lies in the invisibility and imperceptibility of the message [3].

B. Steganography v/s Other Hiding Technique

1. Cryptography v/s Steganography

Steganography and cryptography both are techniques to protect information from unauthorized users but neither technology alone is perfect when the presence of hidden information is revealed the steganography is partly defeated. So the strength of steganography can be amplified by combining it with cryptography. In image steganography the information is hidden in images only [4].

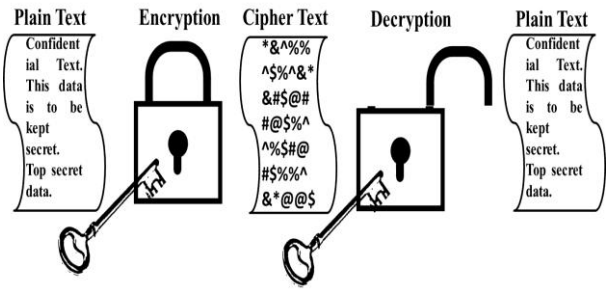

Fig.1 Process of Cryptography

2. Steganography V/S Watermarking

Watermarking is basically done to prevent the illegal copying of the cover object and has an additional requirement of robustness against possible attacks.

DOI 10.17148/IJARCCE.2016.5649

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Steganography system urges to secure embedding of a large amount of information, with no visible degradation to the cover object but watermarking system, however, embeds information that stick to the cover object so hard that it could not be removed or altered without making the cover object entirely unusable [5]. These are vulnerable to illegal copying and regeneration due the advent in the technologies for editing, converting and copying of multimedia. Counter measures are required against duplication and redistribution of digital content [6].

C. Methodology

The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and for randomization in the steganography scheme as in Fig.1In summary:

Secret message + carrier + steganography key= Steganography in medium

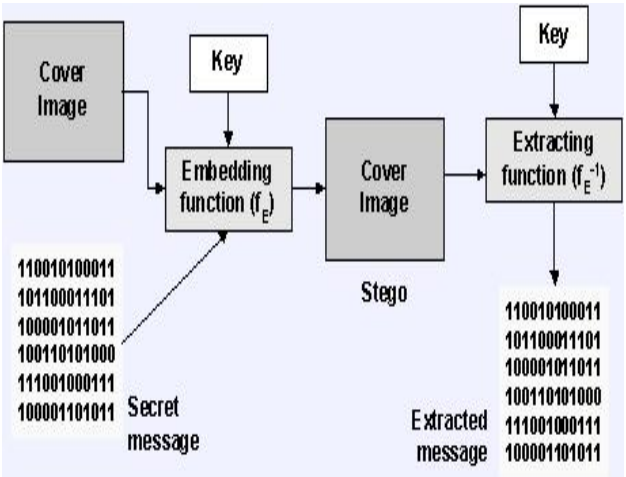

Fig.1 Block diagram of process of Steganography

II. LITERATURE REVIEW

A. Approaches of Steganography Techniques

The continuous growth in data transmission through internet and also the methods which is been developed by the hackers in recent years forced developers to developed more reliable techniques of steganography. There are several techniques of digital steganography. But steganography techniques are mainly categorized in two types [7].

1. Spatial Domain Techniques
2. Transform Domain Techniques

Image steganography in Spatial Domain

In Spatial domain techniques of Image we deals with the Image plane itself in that all the operations on image are done on the pixel value of the image. We know that the image is combination of pixels (x,y), Where x denotes the pixel position in X axis and y denotes the pixel position in Y axis.The Steganography techniques of spatial are less complex and high payload .They cannot even withstand low pass filtering and common image processing attacks. The most Common technique of under Spatial domain is Least Significant bit [8].

LSB (LEAST SIGNIFICANT BIT)

Continuous research in Steganography developed so many algorithms for invisible digital steganography. The simplest algorithm is Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is replaced with a embedding image bit..In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image [9]. All these techniques were based on the pixel value's modifications of the image called Least Significant Bit (LSB).

When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden[10]. With a well chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.

In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect [11]. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key [12]. In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels are not often used on the Internet and might arouse suspicion [13].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Advantages of LSB Image Steganography
1. Easy to implement.
2. Payload capacity is high for 4-LSB embedding.

Disadvantage of LSB Image Steganography:
1. It is lowest robust against statistical analysis of secret information.
2. Low Robustness against visual attacks for higher LSB (3-lsb, 4-lsb methods) embedding.
3. It results in stego-images that contain hidden data yet appear to be of high visual fidelity.

Image steganography in Transform Domain
Transformed domain based steganography are more robust as compared to simple spatial domain steganography. Such algorithms are robust against simple image processing operations like adjustment (contrast and brightness) blurring, low pass filtering, etc. They all are little complex to implement.
Types:
1. Discrete Cosine Transform (DCT)
2. Discrete Wavelet Transform (DWT)

III. PROPOSED WORK

A. Proposed Technique
It is concluded from the research that many embedding image are embed in the HL sub band (Vertical Sub band) and HH sub band (Diagonal sub-band) of the detail coefficients of wavelet transform for maximize robustness against statistical attacks and robustness against visual attacks or imperceptibility.

Coefficients of HH sub band of a level of DWT are selected for embedding image embedding for achieving better the robustness against Gaussian noise attack, cropping attack and Salt & Pepper Noise attack without distortion in quality of image.
After this, on the set of determined HH coefficients of wavelet transform, Discrete Cosine Transform is applied and embedding image is embedded using interchanging of Mid-band coefficients. The detailed steganography embedding procedure of proposed technique is explained as following.

For achieving better imperceptibility with robustness against statics attacks, a combined DWT – DCT technique may be proposed in such a order which have higher PSNR value.

B. Embedding Algorithm of Proposed Hybrid DWT- DCT Steganography Technique

Step 1.Discrete Wavelet Transformation is applied on cover image for decomposing into sub-bands i.e. LL1, HL1, LH1, and HH1 sub-bands.

Step 2. Discrete Wavelet Transformation is applied again on all above sub-bands for decomposing into 16 sub-bands and four HH2 (HH sub-bands at level 2) sub-bands are selected.

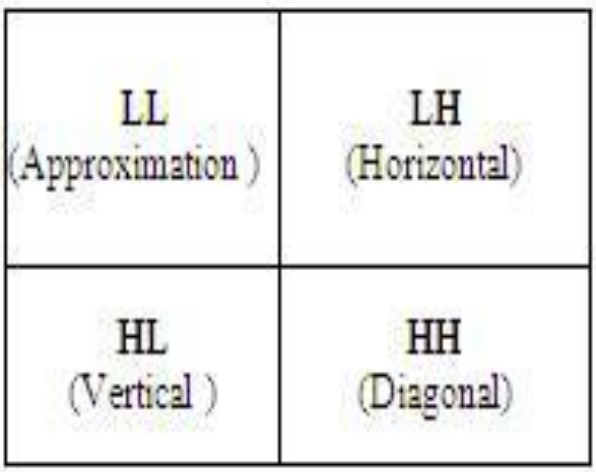

Fig.2 DWT Sub-bands

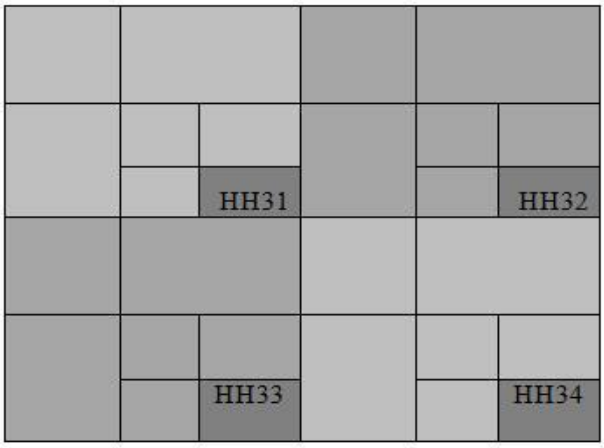

Fig.3 Required DWT Sub-bands for Proposed Hybrid Technique

Step 3.Discrete Wavelet Transformation is applied again on selected four HH2 sub-bands for decomposing into 16 sub-bands and four HH3 (HH sub-bands at level 3 i.e. HH31, HH32, HH33 and HH34 sub-band) sub-bands are selected. These diagonal coefficients (HH sub-bands) are selected achieving better imperceptibility and robustness in order to achieve least distortion in cover image in embedding of secret Image.

Step 4.Perform Discrete Cosine Transform at 8x8 block level on all above selected HH3 sub-bands and 3x3 blocks of DWT-DCT domain is achieved.

Step 5.Embedding image is converted into binary format and bits of DCT coefficients of blocks of above selected sub band are modified with bits of secret image.

Step 6.Apply inverse Discrete Cosine Transform on each bock.

Step 7.Apply inverse Discrete Wavelet Transform to get secret image embedded image.

C. Extraction Technique of Proposed Hybrid DWT - DCT Steganography Technique
The proposed hybrid DCT-DWT secret steganography technique is a blind technique of steganography so the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

original cover image is not needed to extract the secret image. The decoding procedure is mentioned as follows:

Step 1.Discrete Wavelet Transformation is applied on secret image for decomposing into sub-bands i.e. LL1, HL1, LH1, and HH1 sub-bands.
Step 2. Discrete Wavelet Transformation is applied again on all above sub-bands for decomposing into 16 sub-bands and four HH2 (HH sub-bands at level 2) sub-bands are selected.
Step 3.Discrete Wavelet Transformation is applied again on selected four HH2 sub-bands for decomposing into 16 sub-bands and four HH3 (HH sub-bands at level 3 i.e. HH31, HH32, HH33 and HH34 sub-band) sub-bands are selected. These diagonal coefficients (HH sub-bands) are selected achieving better imperceptibility and robustness in order to achieve least distortion in cover image in embedding of secret image.
Step 4.Divide the sub-bands HH31, HH32, HH33, HH34 in 8x8 blocks.
Step 5.Reconstruct the image of secret image using extracted Bits from secret imaged image.

IV. ANALYSIS OF PROPOSED WORK

A. Experiments
The Experiments of Proposed Hybrid DCT-DWT image steganography technique is performed on host images of Lena, and Elaine of size of 512x512 pixels each. A secret image image of size of 32x32 binary image as shown in the figure is embedded as secret image in host images.

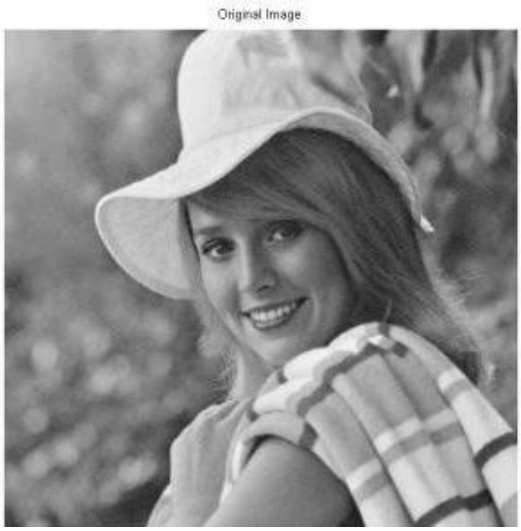

Fig.4 Sample Cover image

B. Performance Matrix
Measurement units for capacity of secret information which can be embedded in cover image, imperceptibility of secret data and robustness against attacks is defined as following.
Payload Capacity: Payload Capacity is amount of data of cover image which is possible to embed with secret information. It can be measured either in percentage of cover image or in average bits per pixel.

Imperceptibility: Imperceptibility means that the distortion or changes in quality of the host or cover image due to embedding of secret image should not be perceived. The imperceptibility is measured mathematically in terms of weighted Peak signal to noise ratio (WPSNR) and Peak signal to noise ratio (PSNR).
Due to embedding the digital cover image is distorted due to changes of pixel value so Quality of stego image after the embedding of secret information should be Robustness against visual Attacks, which is called imperceptibility of secret information which is Proportional to PSNR (Peak Signal to Noise Ratio) as defined in equation 1.

$$PSNR = 10 * \log (P^2/MSE) \quad (1)$$
$$MSE = (1/MN) \sum_i^m \sum_j^n (Wij - Hij) \quad (2)$$

Where P: - Max. Value in Cover Image
Wxy: value of pixel at position i,j in embedding image
Hxy : value of pixel at position i,j in Host Image.
M & N are the pixels in rows & column of Cover image respectively.

A higher PSNR value indicates that the embedding image closely resembles the original image. Generally, if PSNR value greater than 35 dB the secret image is within acceptable degradation level that is the secret image is invisible to human visual system.
Robustness: For robustness, the Mean absolute error (MAE) is measured between the original secret image and corresponding extracted secret image after applying different signal processing attacks over the secret image. A lower MAE value shows that the extracted secret image resembles the original secret image closely.

Implementation
To evaluate the capability of proposed Hybrid algorithm for secret image we design the code in MATLAB 2008a and implements it with the GUI that's helps everyone to understand this concept easily.
For comparing results we take the cover image & secret image as taken by Vijaya K. Ahire, Vivek Kshirsagar[15] The Experiments of Proposed Hybrid DCT-DWT image steganography technique is performed on cover image of Lena of size of 512x512 pixels. A secret image of size of 32x32 binary images as shown in the Fig.5 is embedded as secret image in above host image.


Fig.5 Secret image for Experiment

C. Experimental Run
The step by step working of proposed system is as follows:
Step 1: Click on the stego m file in MATLAB. Then a GUI comes out:
Step 2: Click on the Browse cover image button, it opens the browse window to select cover image:
Step 3: Select input image as your choice.for our experiment we selected lena image of 512*512 pixels.

DOI 10.17148/IJARCCE.2016.5649

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

After that selection one window opens shows the selected image.

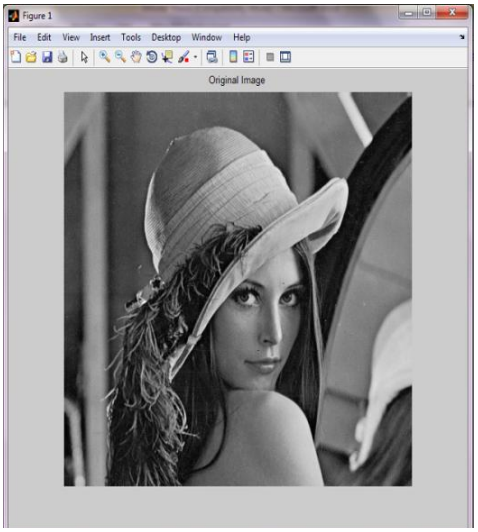

Fig.6 Cover Image Lena 512*512

Step 4: After this secret image is embedded which embed secret image logo into cover image according to the Proposed Algorithm.
Stego image is shown as following:

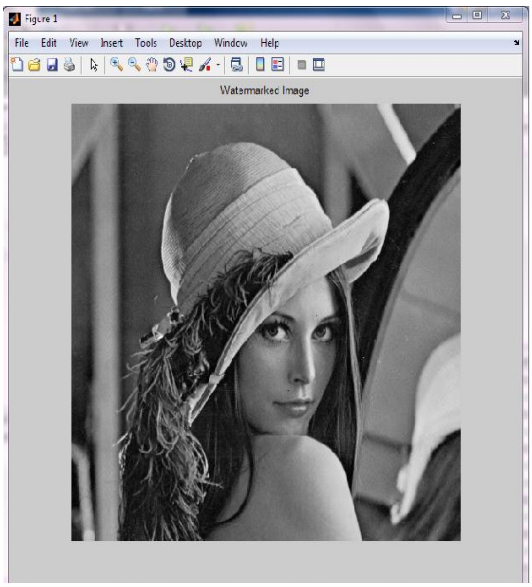

Fig.7 Stego Image Lena

D. Results
As we a take the reference of by Vijaya K. Ahire, Vivek Kshirsagar[15] so results should be compare with their results.The results of PSNR and MAE for the proposed hybrid algorithm in table 1.

Table 1: Results of digital image steganography using proposed hybrid DCT-DWT technique

S no	Image Name	PSNR
1	Leena	44

Table 2: Results of digital image steganography algorithm by Vijaya K. Ahire, Vivek Kshirsagar[15]

S no	Image Name	PSNR
1	Leena	39.2

Input and Output Images are:

Fig.8 Cover Image

Fig.9 Stego Image

Input and Output embedded image are:

Fig.10 Original embedded image Logo

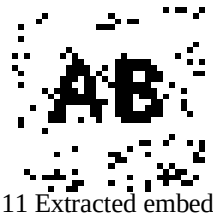

Fig.11 Extracted embedded image Logo

E. Analysis of Results

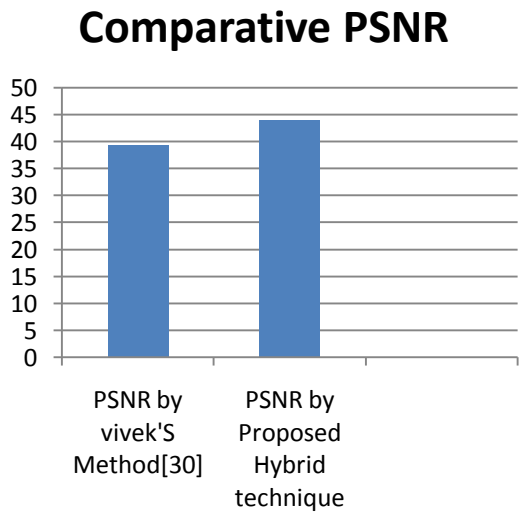

Fig.12 Analysis graph of PSNR of proposed technique and other technique

DOI 10.17148/IJARCCE.2016.5649

Table 1 & 2 and Fig. 10 shows the comparative PSNR value of proposed method and vijaya & vivek method. From the results it is derived that proposed technique achieved PSNR value 44 while vijaya & vivek's method provide PSNR 39.2. So proposed method achieved PSNR more than vijaya's method. PSNR signifies robustness against visual attack for invisible steganography. So proposed technique have higher imperceptibility or higher robustness against visual attacks.

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

The Proposed algorithm presents Hybrid DCT-DWT Digital image steganography algorithm. Proposed method exploits strength of two combined transform domain techniques DCT & DWT to obtain further imperceptibility and robustness. The idea of inserting embedding image in combined transform is based on fact that joint transform eliminates drawback of each other and thus an effective embedding image method can be obtained. Proposed Approach embedding image is embedded is imperceptible part of an image than other methods as shown in results. Steganography is done by embedding image in middle frequency coefficient set of the 3-level DWT transform of host image followed by block level Discrete Cosine Transform and selected HH Discrete Wavelet Transform coefficient sets. So this algorithm seems better than the other approach result shown in results.

From the results it is derived that proposed technique achieved PSNR value 44 while vijaya&vivek 's method provide PSNR 39.2.So proposed method achieved PSNR more than vijaya's method. PSNR signify robustness against visual attack for invisible steganography. So proposed technique has higher imperceptibility or higher robustness against visual attacks.

B. Future Work

Proposed technique can be modified with cryptography and different types of attack can be performed on proposed technique and performances are calculated against attacks.

REFERENCES

[1] Arvind Kumar, Km. Pooja,"Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[2] S.B. Shadkhan, "Cryptography:currents status & future trends", International Conference On Information & Communication Technology: from Theory to Applications, IEEE, pp:417-418, 2004.

[3] R.Anderson and F. Petitcolas, "On the limits of steganography" International Journal of Selected Areas in Communications,IEEE, Vol. 16, No. 4, pp. 474-481, 1998.

[4] A.I. Hashad, A.S. Madani, A.E.M.A. Wahdan, "A robust steganography technique using discrete cosine transform insertion", Third International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society, IEEE, pp. 255-264, 2005.

[5] T. Liu and Z. Qiu, The survey of digital watermarking-based image authentication techniques, 6th International Conference on Signal Processing, vol. 2, pp. 1556- 1559, Aug. 2002.

[6] F.P. Gonzales and F. R. Hernandez, A Tutorial on Digital Watermarking, IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology, pp. 286-292, Oct. 1999.

[7] S. Katzenbeisser and F.A.P. Petitcolas,"Information hiding techniques for steganography and digital watermarking", Artech House Publishers, 2000.

[8] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking". Journal of Computer Science, pp. 740-746, 2007.

[9] S.A. Kasmani and A.N. Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08, vol. 2, pp. 539-544

[10] M. Zhao and Y. Dang, "Color Image Copyright Protection Digital Watermarking Algorithm Based on DWT DCT", IEEE.

[11] C.C. Chang, Y.Z. Wang and C.S. Chan, "An Efficient Probability-Based t out of n Secret Image Sharing Scheme", Second International Conference on Future Generation Communication and Networking Symposia, 2008. FGCNS '08., vol.3, pp.121-124, 2008.

[12] A.R. Calderbank,I Daubechies, w. sweldnens,B. Yeo, " Wavelet transforms that map integers to integers" applied and computational harmonic analysis, vol. 5, pp 332- 369,1998.

[13] G. xuan, J. Zhu, Y. Q. Shi, Z.Ni and W.Su., "Distortion less data hiding based on integer wavelet transform", IEEE , pp.1646-1648, 2002

[14] Vijay Kumar, Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography", International Conference on Advance Computing, IEEE, 2010.

[15] Vijaya K. Ahire, Vivek Kshirsagar ,"Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.

BIOGRAPHIES

Ms. Anuradha Goswami is M.Tech scholar in CSE from Rajasthan Technical University, Kota (GITS, Udaipur).

Ms. Sarika Khandelwal is an Asst. Prof. M.Tech Dissertation guide in GITS, Udaipur. She done M.Tech from U.P. Technical University, Lucknow and her domain of research includes Biometric security & soft computing.

DOI 10.17148/IJARCCE.2016.5649